

# Pipeline

Knowledge Is Power

[www.pipelinepub.com](http://www.pipelinepub.com) Volume 5, Issue 5

## Gateway to Traffic Intelligence Providing Intelligence for Traffic Management & Security

By Dr. Antonio Nucci

Managing and securing large IP networks has become nothing short of a nightmare for network operators due to their increasing complexity. Defending against a gamut of innovative and sophisticated network attacks adds to the complexity, making it harder for operators to effectively deliver value-added services to increase business revenue. Operators tend to install *silo* applications to address specific network problems, resulting in inefficient business operations.

However, operators are turning to a new concept in which their existing infrastructure investments are leveraged and combined with security and traffic management solutions to create a complete *system* – a gateway to traffic intelligence.

### Common Solutions for Managing and Protecting IP Traffic

Historically, operators have purchased siloed applications and installed them incrementally to address specific needs, each of them deployed to solve a specific problem. This practice led to a dispersion of information across many products that do not interact with each other, and a large operational investment to manage and maintain this complex infrastructure.

Operators most often use deep packet inspection (DPI) for traffic management, and a wide range of solutions for traffic security, including firewalls, intrusion detection systems (IDSs), security event managers (SEMs), and network behavior anomaly detection (NBAD).

DPI provides visibility and control of protocols, services, and applications, but its intelligence is confined to inspecting one link at a time and is therefore unable to provide visibility of the traffic from a network-wide perspective. As DPI vendors are asked to handle increasingly faster speeds, content inspection and data analysis are sacrificed. DPIs are limited in their abilities to parse entire packet payloads and act as forensic devices, and are unable to process data with sophisticated algorithms that are required to deal with present and future threats.

In terms of security, many shields of defense are needed and thus deployed in

today's networks, such as firewalls, IDSs, SEMs, and NBAD. Firewalls examine incoming or outgoing packets and allow or disallow their transmission or acceptance on the basis of a set of configurable rules, called policies. Although firewalls represent an indispensable shield to deploy, they require knowledge of attacks in order to be effective, and thus are vulnerable to zero-day threats and sophisticated attacks. Furthermore, they have no visibility into the attack preparation, propagation, result and identity of the attacker.

IDSs detect unwanted manipulations of end hosts; several types of malicious behaviors such as network attacks against vulnerable services; data-driven attacks on applications; host-based attacks, such as privilege escalation, unauthorized logins and access to sensitive files; and malware. Although IDSs are capable of detecting zero-day attacks, they still do not provide visibility into attack preparation, propagation, intent, identity, and effectiveness. SEMs enable SOC efficiency by correlating dispersed and unassociated security events. An SEM system allows the operator access to all logs through a consistent central interface. The events can be parsed for significance as they hit the SEM, and alerts and notifications can be immediately sent out to interested parties as warranted. Unfortunately, SEMs provide only basic correlation using security events, logs, and SNMP traps. Current SEMs are not designed to process millions of events per second, as they were designed and built for enterprise networks.

How is the RCS evolving the IMS ecosystem? Find out at...



**IMS**  
GLOBAL CONGRESS 2008  
1st-4th December, Munich

Book online at [www.ims-congress.com](http://www.ims-congress.com) and quote **CG2465PIPE**

Finally, NBADs enable SOC efficiency by correlating and analyzing raw traffic flows and routing events, and are complementary to an SEM system. NBADs are capable of detecting a wide range of abnormalities and threats targeting data and routing, and are designed to correlate and process millions of events per second in real-time. Due to the wider and more complete view of the traffic activity and the associated network responsiveness, the NBAD system provides a unique insight into the attack preparation, propagation, and real breadth of the attack. Unfortunately, current NBADs are solely based on SNMP data, traffic flow records and routing events. They lack the deep visibility into traffic packets (as offered by DPI), the flexibility in creating customer policies (as offered by firewalls) and the knowledge of the attacker's identity.

Each of these solutions brings something novel and important from an operational perspective, either as a useful tool to better manage the traffic itself or as a fundamental security shield against an ever-growing number of threats. Although each of these products is needed to carry out a specific type of analysis and function, a system that leverages the strengths of each can dramatically improve operational efficiencies. A system that can correlate and analyze all the information captured and processed, interpret and cluster associated alerts, and manage the overall infrastructure as a whole (monitor, diagnose, act on the data collected from a large pool of such solutions) from a single console is even more powerful. This type of system is truly a "Gateway to Traffic Intelligence" (GTI).

### **Characteristics of a Comprehensive GTI System**

A comprehensive GTI system is designed to offer a series of fundamental operational values that ensure a secure, scalable, and high-performance network. Firstly, it offers deep insight into the behavior of network protocols, applications and services from a network-wide perspective. With a GTI system in place, the operator has the ability to understand which services, applications, and even end users consume the most bandwidth, along with the performance metrics with which services are delivered. This function is typically provided by today's DPI products at a network link level. With a GTI, the operator is able to extend this knowledge to many links at the same time, thus gaining the global "network-wide" perspective.

The system also offers flexible normalization, scalable correlation and sophisticated statistical analysis of multi-typed information. It leverages the network infrastructure to provide the operator with 24/7 traffic monitoring and a prompt detection of traffic abnormalities. Such events are displayed with enriched records of information to enable the operator to carry out a thorough, easy and guided troubleshooting process.

A comprehensive GTI system provides extensive forensic analysis of traffic abnormalities, facilitated by close interaction with the underlying network infrastructure. It enables the operator to understand the nature of the anomaly; the life-cycle of the anomaly; the impact of such anomaly to protocol, services and applications being delivered (in terms of QoS) and customers affected (in terms of service-level agreements, or SLAs); the packet-payload; and the data, all by providing a fast query engine and extensive reporting to organize and distill data as required.

Powerful contextualization of information for easy identification of the cause of the problem is essential to a GTI system, as well. Usually, a problem manifests itself in many different shapes and forms. One problem can generate tens or even hundreds of alerts, making the troubleshooting process time-consuming for the operational personnel. The GTI system distills the vast amount of information, clusters alerts associated to the same problem, and pinpoints the cause of the problem for the operator. The operator is then able to take prompt action against the cause of the problem, thus saving precious time and diminishing the negative impact of the problem to the network and the associated customer perception.

A comprehensive GTI system offers the operator a complete view of the anomaly and provides a vast set of actions from which to choose. The system has an

inherent ability to identify which actions can be executed on a given network element, which elements the operator should act on, and guides the operator as to what kind of actions to take.

**A** GTI system is also able to scale depending on the size of the network. It has the ability to process large volumes of data captured from many network elements in real-time.

Finally, a GTI system is highly modular, easy to manage to accommodate fast integration with third-party network infrastructure, and substantially cuts operational costs. It provides open south- and north-bound APIs to facilitate the collection and policy enforcement from and to a variety of different network elements.

### **GTI Demystified: Breakdown of Sources**

Operators must collect and analyze data from a wide variety of sources in order to keep their networks secure and operating efficiently, including packet and flow statistics, SNMP statistics, firewall/NAT/AAA events, routing and topology events, and IP-SLA metrics. Each source of data brings immense value to a GTI system.

Telemetry and SNMP are two fundamental and rich sources of data for gaining a good understanding of the health of the traffic and network elements. They constitute the basic foundation of traffic intelligence. Telemetry from routers is a powerful source of information used today to gain a global view of the network activity at the Layer-4, or flow, level. Since operators can enable sampling, telemetry is the de-facto source of data used to monitor traffic activity across the entire network. The system that consumes telemetry data can provide the operators with details on the nature of the traffic flowing across the entire network and its overall composition. Only very recently, routers have been equipped with more powerful functionalities that go beyond the Layer-4 information. Indeed, such routers can export packet level records on demand for forensic analysis. SNMP statistics captured from routers and router interfaces enable a more accurate assessment of the impact of traffic abnormalities to network elements in terms of volume and element health.

Layer-7 data from DPI appliances is used for traffic management. It is indispensable for a very accurate breakdown of traffic into network protocols, services, and applications. When Layer-7 information is collected from many links, correlated and analyzed in a central location, the operators gain a unique network-wide perspective into their services and applications. DPI appliances can be used as intelligent and targeted mitigation devices in case the operator is willing to take surgical actions on a per-packet basis.

Routing (BGP, IGP) and topology information is fundamental to understanding how packets traveled into the network and which network elements they have traversed. Operators can pinpoint the network element that caused the problem and act on it. Routing information is essential to monitor the stability of the routing infrastructure, and to detect router misconfiguration and threats targeting the overall routing infrastructure.

SLAs determine the type of service the provider guarantees, and the monetary impact when the service level is violated. A GTI system can quantify the impact of security events on customers and service using the existing technology in network equipment.

Firewalls/NAT/AAA provide broad coverage of a variety of attacks either from legitimate sessions with unauthorized users or legitimate sessions that violate a customer's policies. A GTI system combined with a firewall/NAT/AAA will provide additional visibility into end-host and user credentials, beyond public IP to private IP (NAT translation) and user credentials. The integrated solution will enable the operator to understand the threat impact and intent.

### **Contextualization of Information**

A side-effect of the increasing complexity and size of today's networks is the increase in the volume of alerts associated with anomalous or malicious traffic. In fact, a single malicious anomaly can generate up to 40 individual alerts, all of which are related to the same cause. An effective GTI system offers a way to group these related alerts into "meta-events" in an effort to slim down that mass of information into a manageable form. The individual alerts are still available, but with a GTI system, NOC/SOC personnel can maximize resources by focusing on the associated cause. This same logic is also applied to BGP updates, which are commonly reported in terms of their volumes over time. With a GTI system, BGP updates associated to the same cause of the problem are turned into "BGP events" that are addressed in groups and linked to the cause of the problem. As a result, the operator will have only tens of BGP events per day to review, rather than hundreds or thousands. At the same time, GTI provides deep insight into the cause of those events, alerting the operator as to which of those changes might affect the normal operation of their network. Overall, the ability to summarize information while still allowing for drill-down capability ensures that security groups are efficient in their analysis and effective in their mitigation practices.

### **Measure Impact to Network Protocols, Services, and Applications**

Detecting the presence of a network problem (normal or malicious) without a deep understanding of the effects to the QoS of the services and applications involved is meaningless to network operators. What matters the most to an operator is satisfying the SLA signed with their customers by meeting the QoS metrics. Consequently, a GTI system must provide visibility into QoS metrics for SLA compliance. A GTI system captures, creates, and profiles IPSLA metrics used to monitor the correct behavior of network protocols, services, and applications. Those metrics such as RTT, jitter, packet losses, and Layer-7 SLA metrics specific to the most used protocols are generated either using information collected from DPI appliances or by a close interaction with network routers whose IOS supports such functionality. When any of the metrics being baselined violate a specific criteria being configured by the operator, an alert is triggered and detailed reports are displayed. Operators might decide to prioritize their tasks by using this metric as an example (since it is the one they measure as a source of revenue with their customers).

## **Real-Time Forensic Analysis**

Forensic analysis is another key feature of a GTI system. Operators must have a converged operational view across the network traffic, routing, topology, service, and application behavior. The operator must access tabular and graphical reports before, during, and after a problem has occurred and corrective action has been taken. A GTI system allows an operator to dig deeper into an alert detected by close interaction with DPI boxes or routers that have seen the malicious stream. Raw flow and packet information can be captured and extensively analyzed by security personnel.

The GTI system provides two ways for the operator to carry out the forensic task: passive or active. Passive forensic analysis allows the operator to store flow and packet records in an external database. Active forensic analysis, also known as forensic on-demand, allows the operator to retrieve information directly from the network as required.

## **Suggest Where and How to Take an Action**

As part of their duties, operators must be in a position to react to a problem quickly and precisely. This means that the GTI system has to pinpoint to the operator which network elements have seen the anomaly being detected and suggest which network element to act on in order to resolve the problem promptly and with minimal network intrusion. Thus, the GTI system must guide the operator through the entire troubleshooting process. It must monitor in real-time the effectiveness of the action put in place in the network and create reports for the operator. The GTI system provides a vast pool of actions that can be taken, ranging from policy enforcement to specific appliances, or automated generation of ACL, or blackholing and sinkholing, or integration with third-party mitigation devices.

## **Scalability**

The GTI system is designed to meet scalability requirements of operators. It can incrementally scale to support changes in traffic volume, number of events, and network coverage. While each collector can collect up to 150,000 events per second, the system can load balance across additional modules to collect and process traffic from as many points in the network as required. The GTI system can process millions of events per second in real-time by using sophisticated load-balancing algorithms to spread the load across the available servers. Similarly, it uses parallel data streams algorithms designed to process a voluminous amount of data and data reduction techniques.

## **In Conclusion**

Operators now regard the ability to see every bit of information traversing their network not only as a potential source of revenue, but also as a key differentiator in the market to deliver advanced services in the most reliable manner. As a consequence, from a service provider's perspective, efficient traffic management is imperative. In other words, the reliability and efficiency with which ISPs deliver

content to their customers and the protection of every single bit of information is a major differentiator that enables them to attract new customers and decrease operational cost. Using a GTI system will make achieving this differentiator easily attainable.

***If you have news you'd like to share with Pipeline, contact us at [editor@pipelinepub.com](mailto:editor@pipelinepub.com).***

Not for distribution or reproduction.